Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] What is claimed is:

1.A method for decrypting data received by a receiver, the receiver being in communication with a sender, comprising:

receiving the encrypted data from the sender;

searching a key-table of the receiver for a decryption key corresponding to the encrypted data;

updating the key-table according to the encrypted data and enabling a re-transmission mechanism of the sender when the decryption key is not stored in the key-table;

decrypting the encrypted data through utilizing the decryption key stored in the key-table.

[c2] 2.The method of claim 1 further comprising using a Media Access Control (MAC) Address of the sender to search the key-table for the decryption key.

[c3] 3.The method of claim 1 further comprising triggering a system interrupt to notify a controller of the receiver if the decryption key is not stored in the key-table.

[c4] 4.The method of claim 3 wherein the controller searches the master list for the decryption key and transfers the

decryption key to the key-table when receiving the system interrupt.

[c5] 5.The method of claim 1 further comprising replacing a least frequently used decryption key in the key-list with the decryption key transferred in.

[c6] 6. The method of claim 1 further comprising discarding the encrypted data when the decryption key is not stored in the key-table.

[c7] 7.The method of claim 1 wherein the step of enabling a re-transmission mechanism comprises disabling the receiver from outputting an acknowledgement message to the sender to inform the sender of reception of the encrypted data.

[c8] 8.The method of claim 1 being applied to a wireless LAN (WLAN) system.

[c9] 9.The method of claim 1 wherein the receiver is a wireless network card inserted in a computer.

[c10] 10.A method for decrypting data received by a receiver, the receiver being in communication with a sender, comprising:
receiving an encrypted data from the sender;
disabling an acknowledgement message which informs

the sender of reception of the encrypted data and updating the key-table according to the encrypted data when a decryption key is not stored in a key-table, wherein the decryption key corresponds to the encrypted data;
receiving an re-transmitted encrypted data from the sender; and
decrypting the encrypted data re-transmitted from the sender through utilizing the decryption key stored in the key-table.

[c11] 11.The method of claim 10 further comprising using a Media Access Control (MAC) Address of the sender to search the key-table for the decryption key.

[c12] 12. The method of claim 10 further comprising replacing a least frequently used decryption key in the key-list with the decryption key transferred in.

[c13] 13. The method of claim 10 being applied to a wireless LAN (WLAN) system.

[c14] 14. The method of claim 10 further comprising discarding the encrypted data when the decryption key is not stored in the key-table.

[c15] 15. The method of claim 10 wherein the sender re-transmits the encrypted data if the sender does not receive the acknowledgement message, and the receiver

decrypts the encrypted data re-transmitted from the sender.

[c16] 16. An apparatus for decrypting data received by a receiver, the receiver being in communication with a sender, comprising:
a key-table for storing a plurality of decryption keys; and
a receiving controller, coupled to the key-table, configurable to
receive an encrypted data from the sender,
search the key-table for a decryption key corresponding to the encrypted data, enable a re-transmission mechanism of the sender when the decryption key is not stored in the key-table, and
update the decryption keys in the key-table according to the decryption key when the decryption key is not stored in the key-table.

[c17] 17. The apparatus of claim 16 wherein the receiving controller discards the encrypted data when the decryption key is not stored in the key-table.

[c18] 18.The apparatus of claim 16 wherein the receiving controller uses a Media Access Control (MAC) Address of the sender to search the key-table for the decryption key.

[c19] 19.The apparatus of claim 16 wherein the receiving con-

troller replaces a least frequently used decryption key in the key-list with the decryption key transferred in.

[c20] 20. An apparatus for decrypting data received by a receiver, the receiver being in communication with a sender, comprising:
a key-table for storing a plurality of decryption keys; and
a receiving controller, coupled to the key-table, configurable to
receive an encrypted data from the sender,
search the key-table for a decryption key corresponding to the encrypted data,
disable an acknowledgement message which informs the sender of reception of the encrypted data when the decryption key is not stored in the key-table, and
update the decryption keys in the key-table according to the decryption key when the decryption key is not stored in the key-table.